



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/262,123	03/03/1999	DAVID CARROLL CHALLENGER	RP9-98-089	8958

7590 12/04/2001

ANDREW J DILLON
FELSMAN BRADLEY VADEN GUNTER AND DILLON
SUITE 350 LAKEWOOD ON THE PARK
7600B NORTH CAPITAL OF TEXAS HIGHWAY
AUSTIN, TX 78731

[REDACTED] EXAMINER

ZAND, KAMBIZ

[REDACTED] ART UNIT [REDACTED] PAPER NUMBER

2132

DATE MAILED: 12/04/2001

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/262,123	CHALLENER ET AL.	
	Examiner Kambiz Zand	Art Unit 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 03 March 1999.
- 2a) This action is FINAL. 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-17 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) Claim(s) _____ is/are allowed.
- 6) Claim(s) 1-17 is/are rejected.
- 7) Claim(s) _____ is/are objected to.
- 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on 03 March 1999 is/are: a) accepted or b) objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- 11) The proposed drawing correction filed on _____ is: a) approved b) disapproved by the Examiner.
If approved, corrected drawings are required in reply to this Office action.
- 12) The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

- 13) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) All b) Some * c) None of:
1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.
- 14) Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).
a) The translation of the foreign language provisional application has been received.
- 15) Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

- | | |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) Paper No(s). _____ |
| 2) <input checked="" type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ | 6) <input checked="" type="checkbox"/> Other: <i>Petition</i> |

DETAILED ACTION

1. Claims 1-17 have been examined.

Information Disclosure Statement PTO-1449

2. The pages of the all references in English submitted by applicant have been considered.

Drawings

3. New formal drawings are required in this application because original drawings by the applicant were objected to by the Draftsperson under 37 CFR 1.84 or 1.152. Please see attached PTO-948. Correction is requested.
4. Figures 1 should be designated by a legend such as --Prior Art-- because only that which is old is illustrated. See MPEP § 608.02(g).
5. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they do not include the following reference sign(s) mentioned in the description Page 10, lines 26 and 28; items "30" and "262". Correction is required.
6. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(4) because reference character "204" in fig. 2 has been used to designate both PCI bus bridge and ISA bus bridge (see page 8, lines 8 and 11).
Correction is required.

Claim Rejections - 35 USC § 102

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) The invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

8. Claims 1-17 are rejected under 35 U.S.C. 102(e) as being anticipated by Boneh et al. (6,134,660).

As per claims 1 and 9 Boneh et al. (6,134,660) teach a method and a system in a data processing system for maintaining secure user private keys in a non-secure storage device, said method comprising the steps of: establishing a master key pair for said system (see col. 6, lines 38-40), said master key pair including a master private key and a master public key (see col. 7, lines 45-47); storing said master key pair in a protected storage device (see col. 7, lines 55-56; fig. 2); establishing a unique user key pair for a user, said a user key pair including a user private key and a user public key (see col. 8, lines 18-27); encrypting said user private key utilizing said master public key; and storing said encrypted user private key in said non secure storage device (see col. 7, lines 50-63; fig. 2), wherein said encrypted user private key is secure while stored in said non-secure storage device (fig. 2, item108).

As per claims 2 and 10 Boneh et al. (6,134,660) teach the method and the system according to claim 1, further comprising the steps of: establishing an encryption device having an encryption engine and said protected storage device; and said protected

storage device being accessible only through said encryption engine (see fig. 3, item 108 through 210).

As per claims 3 and 11 Boneh et al. (6,134,660) teach the method and the system according to claims 2 and 10, further comprising the step of said encryption engine encrypting said user private key utilizing said master public key stored in said protected storage device (see fig. 3, item 204).

As per claims 4 and 12 Boneh et al. (6,134,660) teach the method and the system according to claims 3 and 11, further comprising the steps of: an application generating a message to transmit to a recipient (see fig. 2); said encryption engine decrypting said user private key utilizing said master private key; said encryption engine encrypting said message utilizing said decrypted user private key and a recipient's public key; and said system transmitting said encrypted message to said recipient (see fig. 5B and 6).

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. Claims 5-16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Boneh et al. (6,134,660) in view of McBride (6,292,899B1).

As per claims 5 and 13 Boneh et al. (6,134,660) teach the method and the system according to claims 4 and 12 above, wherein the step of establishing a user key pair as applied to claim 1 above but fail to explicitly point out the step of associating said user key pair with an application. However McBride (6,292,899B1) teaches that relationship (see fig. 3, item 301). It would have been obvious to one of ordinary skilled in the art at the time the invention was made to include McBride (6,292,899B1) method with relation to programs and application in Boneh et al. (6,134,660) system and method in order to provide secure transmission of programs and application in a wide area network environment.

As per claims 6 and 14 Boneh et al. (6,134,660) teach the method and the system as applied to claims 5 and 13 but do not disclose explicitly the steps of: establishing a certificate, said certificate being associated with said application, said user private key, and said user; in response to said user attempting to access said application utilizing said certificate, said encryption engine utilizing said certificate to determine a location within said non secure storage device for said user private key associated with said certificate; said encryption engine decrypting said user private key; and said encryption engine utilizing said decrypted user private key to encrypt messages transmitted by said application. However McBride (6,292,899B1) teaches the above relationship and describes a master file (certificate) associated with the application (see col. 7, lines 7-13; col. 5, lines 40-67). It would have been obvious to one of ordinary skilled in the art at the time the invention was made to include McBride (6,292,899B1) method with relation to use of a master file as a certificate in relation with programs and application in Boneh

et al. (6,134,660) system and method in order to provide highly secure transmission of programs and application in a wide area network environment.

As per claims 7 and 15 Boneh et al. (6,134,660) teach the method and the system according to claims 6 and 15, wherein said step of storing said user private key in said non-secure storage further comprises the step of storing said user private key (see fig. 2-3) but mentions backup tape and not explicitly a hard drive. However it is well known in the art that hard drive are one type of storage device for backing up and storing data. It would have been obvious to one of ordinary skilled in the art to use hard drive as well as other storage medium in order to store different kind of data including backup data.

As per claims 8 and 16 Boneh et al. (6,134,660) teach the method and the system according to claim 7, further comprising the step of said user key pair being capable of being utilized only in said data processing system wherein said user key pair is established as applied to claim 1 above wherein said user key pair is not capable of being utilized in a second data processing system (see col. 6, lines 65-67; col. 7, lines 1-13).

As per claim 17 Boneh et al. (6,134,660) in view of McBride (6,292,899B1) teach a data processing system for maintaining secure user private keys in a non-secure hard drive, comprising: an encryption device including an encryption engine and a protected storage device for establishing a master key pair for said system, said master key pair including a master private key and a master public key, said protected storage device for storing said master key pair, said protected storage device capable of being accessed only through said encryption engine; said encryption device executing code

Art Unit: 2132

for establishing a unique user key pair for a user, said user key pair including a user private key and a user public key, said user key pair being capable of being utilized only in said data processing system wherein said user key pair is established, wherein said user key pair is not capable of being utilized in a second data processing system; said system executing code for associating said user key pair with an application; said encryption device executing code for encrypting said user private key utilizing said master private key stored in said protected storage device; said non-secure hard drive for storing said encrypted user private key, wherein said encrypted user private key is secure while stored in said non-secure hard drive; an application capable of generating a message to transmit to a recipient; said system executing code for establishing a certificate, said certificate being associated with said application, said user private key, and said user; storing said certificate in said non-secure hard drive; in response to said user attempting to access said application utilizing said certificate, said encryption engine executing code utilizing said certificate for determining a location within said non-secure hard drive for said user private key associated with said certificate; said encryption engine executing code for decrypting said user private key; said encryption engine capable of utilizing said decrypted user private key to encrypt messages transmitted by said application; and said system transmitting said encrypted message to said recipient **as applied to claims 1-6 above.**

Conclusion

11. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

Art Unit: 2132

U.S.Patent No. US (4,634,807) teach Software protection device.

U.S.Patent No. US (6,311,270B1) teach Method and apparatus for securing communication utilizing a security processor.

U.S.Patent No. US (5,991,399A) teach Method for securely distributing a conditional use private key to a trusted entity on a remote system.

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kambiz Zand whose telephone number is (703) 306-4169. The examiner can normally reached on Monday-Thursday (8:00-5:00). If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Albert Decady can be reached on (703) 305-9595. The fax phone numbers for the organization where this application or proceeding is assigned are as follows:

After-Final (703) 746-7238

Official (703) 746-7239

Non-Official/Draft (703) 746-7240


Kambiz Zand


ALBERT DECADY
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

11/21/01